ABSTRACT OF THE DISCLOSURE

A connection is established between a server and a web browser having access to a first, trusted public key. The server downloads a digitally signed archive to the browser, the archive including a second public key. The browser verifies the digitally signed archive using the first public key, and stores the second public key in response to the verification. The browser then uses the stored second public key to authenticate the server and establish a secure connection with the server. The second public key and its chain of trust need not be known by the browser beforehand, and the archive may include program fragments that store the key in an area where the browser (or an applet running under the browser) can access and use it. The archive may also include a program fragment that performs certificate validation for the client -- enabling the client to handle certificate types it does not know about. Advantages include allowing the archive to be transmitted over any insecure connection since it is integrity protected and authenticated; and allowing the client to make a direct connection to the server without having to access certificate stores on the platform.